UNCLASSIFIED

AD 401 182

Reproduced
by the

DEFENSE DOCUMENTATION CENTER

FOR

SCIENTIFIC AND TECHNICAL INFORMATION

CAMERON STATION, ALEXANDRIA, VIRGINIA

UNCLASSIFIED

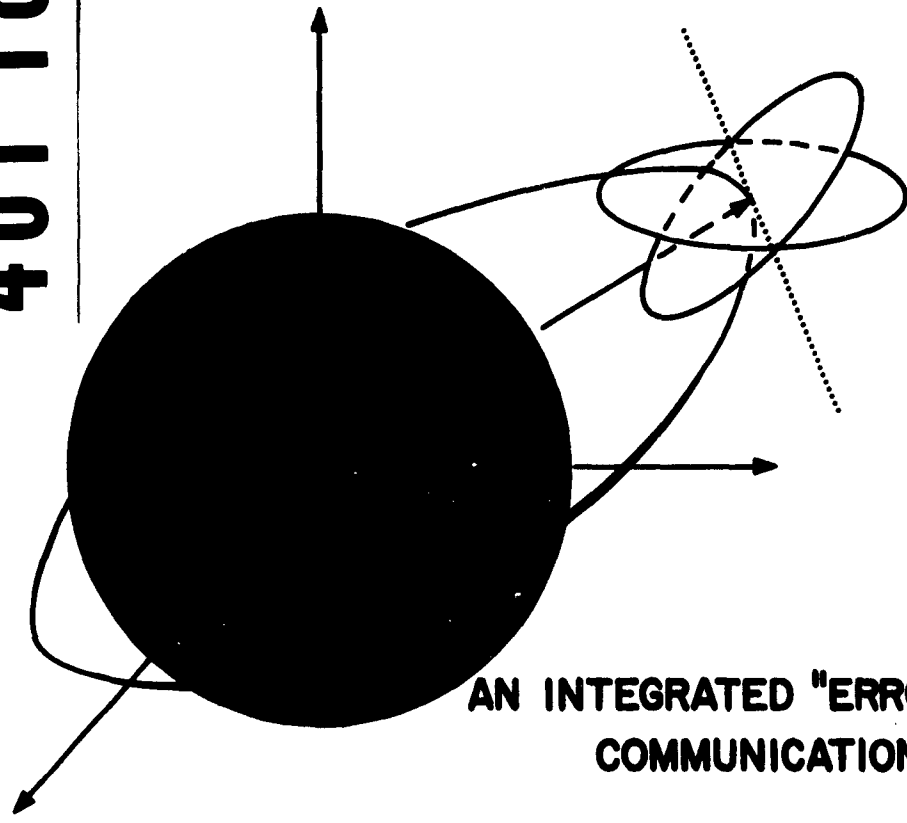
NOTICE: When government or other drawings, specifications or other data are used for any purpose other than in connection with a definitely related government procurement operation, the U. S. Government thereby incurs no responsibility, nor any obligation whatsoever; and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use or sell any patented invention that may in any way be related thereto.

63-3-2

TECHNICAL NOTE

WDL-TN62-13
31 DECEMBER 1962

401 182



AN INTEGRATED "ERROR-FREE" COMMUNICATION SYSTEM

JOHN C. HANSEN
SPECIAL PROGRAMS DEPARTMENT

APR 10 1963
TISIA

AF04(647)-829

PHILCO
A SUBSIDIARY OF Ford Motor Company
WESTERN DEVELOPMENT LABORATORIES

63 2 70

WDL-TN62-13

TECHNICAL NOTE

AN INTEGRATED "ERROR-FREE" COMMUNICATION SYSTEM

Prepared by

John C. Hansen
Special Programs Department

PHILCO CORPORATION
Western Development Laboratories
Palo Alto, California

Definitive Contract AF04(647)-829
AFBM Exhibit 58-1, Paragraph 4.2.1

Prepared for

SPACE SYSTEMS DIVISION
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
Inglewood, California

63 2 .. 70

ABSTRACT

PHILCO WDL-TN62-13 UNCLASSIFIED

AN INTEGRATED "ERROR-FREE" COMMUNICATION SYSTEM

31 December 1962 Pages

Contract AF04(647)-829

This Technical Note presents a code system for extremely reliable information transfer. The system combines the functions of command, synchronization, range, and range rate in one two-way radio link. Reliability results from the use of "comma-free" words coded for error detection, and synchronization has the same high reliability as the information.

THIS UNCLASSIFIED ABSTRACT IS DESIGNED FOR RETENTION IN A STANDARD 3-BY-5 CARD-SIZE FILE, IF DESIRED. WHERE THE ABSTRACT COVERS MORE THAN ONE SIDE OF THE CARD, THE ENTIRE RECTANGLE MAY BE CUT OUT AND FOLDED AT THE DOTTED CENTER LINE. (IF THE ABSTRACT IS CLASSIFIED, HOWEVER, IT MUST NOT BE REMOVED FROM THE DOCUMENT IN WHICH IT IS INCLUDED.)

SUMMARY

In the interests of more efficient operation, a system is proposed which combines the functions of command, synchronization, range, and range rate on one two-way radio link. Extreme reliability of information transfer is achieved by employing "comma-free" words which have been coded for error detection. Consideration is given to an assumed elemental error probability, corresponding to a conservative signal level $P_e = 10^{-4}$. The mean time between error for this case is 10^{14} years. The coding is such that synchronization obtains the same high degree of reliability as the information. In addition to the advantages of essentially "error-free" communication, the system offers relative ease of implementation common to the class of cyclic codes.

FOREWORD

Technical Note WDL-TN62-13 has been prepared by the Philco WDL Special Programs Department for submittal to AFSSD for information purposes. This Technical Note is within the scope defined by Paragraph 4.2.1, AFBM Exhibit 58-1, "Contractor Reports Exhibit," dated 1 October 1959, as revised and amended.

The material presented in this Technical Note was developed under Definitive Contract AF04(647)-829 and Paragraph 1.2.1.2 of AFSSD Exhibit 61-27A, "Satellite Control Subsystem Work Statement," dated 15 February 1962.

AN INTEGRATED "ERROR-FREE" COMMUNICATION SYSTEM

INTRODUCTION

It has become evident in the past few years that the combining of a number of Space Communications functions is both a necessary and profitable course of effort. As the various projects gain in complexity, the number and variety of RF links also increase, resulting in greater weight aboard the vehicle and a corresponding complexity in ground support equipment.

Since the vehicle configuration is usually a Program responsibility and the ground support system a Range responsibility, pressure is exerted on both groups to reduce the number and variety of Space Communications links. Paradoxically, although both groups have the same goal in mind, the Program-oriented group makes the situation worse by its concentrated effort to reduce weight and power requirements. This often results in an ingenious, specialized non-standard airborne system which, in order to be supported, must be matched on the ground by another special equipment system.

This paper advances the proposition that certain functions form a group with two properties: they are universal to all programs, and they are necessary for satisfying the Range support requirements. This group of functions, namely range, range rate, command, and synchronization, can be accomodated in a satisfactory combination on one RF link.

CODING AND SYNCHRONIZATION

In practical systems, both coding and synchronization must be combined. However, in most coding analyses and especially in those which supposedly increase the communication reliability of a particular system, it is always assumed that word synchronization is somehow present. (This might be more confidently assumed for bit synchronization with a reasonable number of zero crossings of the waveform.) Such synchronization is not always present, as can be illustrated by comparing actual

test results with an analysis. Considerable literature on the ways and means of word separation and identification is presently being written as a result of this problem. (Ref. 1,2,3,4,5, and 6)

Cyclic codes* are particularly susceptible in that the code words may be separated by appreciable distances** but a loss or gain of one bit on a time scale can result in another valid code word. There are methods by which it is possible to construct a set D of k letter-code words unique in the property that any overlap between words of D cannot result in another member of D. For example, if

$$(a_1, a_2, \cdots a_k) \text{ and } (b_1, b_2, \cdots b_k)$$

are any two words of the code, then the set

$$(a_2, a_3, \cdots b_1)\cdots(a_3, a_4, \cdots b_2)\cdots(a_k, b_1, \cdots b_{k-1})$$

$$(b_2, b_3, \cdots a_1)\cdots(b_3, b_4, \cdots a_2)\cdots(b_k, a_1, \cdots a_{k-1})$$

is not in D. These so-called "Comma-Free" Codes were advanced as a possible dictionary for Genetic Coding. (Ref. 7)

If all words of periodicity*** less than k are eliminated and if the remaining words are grouped in equivalence classes of cyclic permutations, a dictionary of $W_k(n)$ words results where, for odd k (proved for $k \leq 17$):

---

* A code in which any cyclic permutation of a code word will result in another word of the code.

** Distance between two binary code words is defined as the number of positions in which they differ.

*** For example, the word $(a_1, a_2, a_1, a_2, a_1, a_2)$ has a period of 2.

$$W_k(n) = \frac{1}{k} \sum_{d/k} \mu(d)\, n^{k/d}$$

$$\mu(d) = \begin{cases} 1 \text{ if } d = 1 \\ 0 \text{ if } d \text{ has any square factor} \\ (-1)^r \text{ if } d = P_1, P_2 \ldots P_r \text{ where } P_1, \ldots P_r \\ \quad \text{are distinct primes.} \end{cases}$$

For k = 5 and the binary case of n = 2, the code would appear as follows:

0 1 0 0 0
0 1 1 0 0
0 1 0 1 0
0 1 1 1 0
0 1 0 1 1
0 1 1 1 1

The interesting and desirable property of this code is that there is no need for synchronization between transmitter and receiver since each code word is uniquely decipherable. Further, the task of synch acquisition can never take longer than period k. An undesirable property is evident in error correcting or error detecting: the minimum distance between words is 1, and the code is not systematic*. This can result in unwieldy implementation, which is a decided disadvantage for a space-borne application.

* In a systematic code, the first k symbols are arbitrary information symbols and the last (n-k) check symbols are linear combinations of the first symbols.

By combining the properties of code word distance and ease of implementation peculiar to the class of cyclic codes and the synchronization properties of comma-free codes, it is possible to achieve an essentially "error-free" synchronized communication link. Such a code would then form the basis of the RF link between ground and vehicle from which the various required functions mentioned previously could be derived.

CODE CONSTRUCTION

The code will be constructed for a special case of a typical command link requirement. This will illustrate the method more clearly and will demonstrate that the extension to the general case is immediate. The method of construction is to select a comma-free code of word length k, to code these words in an (n, k) cyclic code possessing the desired error detection or correction properties, and finally, to operate on the (n, k) cyclic code in such a manner as to restore the comma-free property.

The comma-free code will be selected so that it has systematic properties as well as ease of implementation. Both of these properties are included in the so-called "prefix comma-free" codes described by Gilbert. (Ref. 9) The present code will utilize a word length k = 21 with a structure employing the prefix 111110 for each word. A word of the code is therefore represented as:

111110XXXX0XXXX0XXXX0

where the X's represent arbitrary information bits and the 0's ensure the comma-free property. As a result, these words are comma-free and easy to implement.

The set thus obtained may now be encoded in order to provide the necessary error protection. The code chosen, although by no means the only one possible, is the (31, 21) Bose-Chaudhuri code with minimum distance of 5. (Ref. 10) This particular code is optimum for error correction and will detect all combinations of 4 or less errors as well as all burst errors of 10 or less. A burst length is that number of consecutive bits in a word which includes all errors in the word.

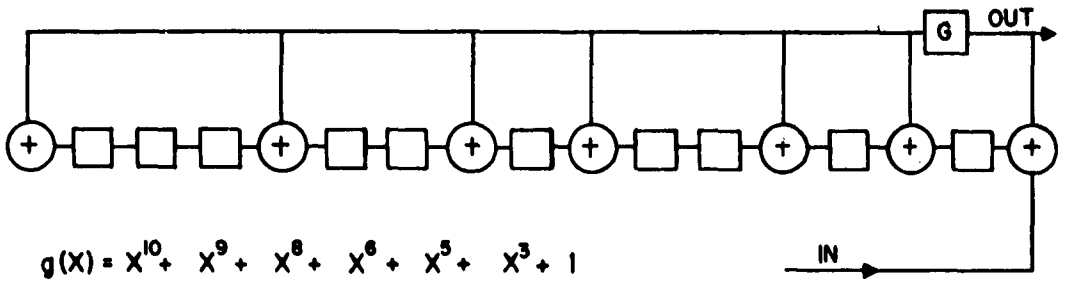
The generator matrix for this code (derived in Appendix A) may be represented as:

$$C^* = \left\| C, I_{21} \right\| \qquad \text{where}$$

$$C = \left\| \begin{array}{cccccccccc} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{array} \right\|$$

As can be seen, the code is in systematic form for ease in coding. The k = 21 bits are the comma-free words and are followed by 10 check bits to make a 31-bit word. This code can be implemented with an (n - k) shift register with the appropriate feedback connections which are derived in Appendix B.

COMMAND ENCODER – DECODER



It now remains to choose a subset of the code such that the comma-free property is not violated. This is most easily accomplished by observing that the check bit sequence is derived for each word by multiplying the matrix C by the particular word to be encoded. Given the comma-free k bit word $(a_1, a_2 \ldots a_k)$, the check bit C_j becomes:

$$C_j = \sum_{i=1}^{k} a_i C_{ij}$$

It is then only necessary to generate two independent parity checks such that the check bit sequence shall have $n(1) < 5$, where $n(1)$ is the number of consecutive 1's in the sequence. For the present example, this is accomplished by generating parity checks such that $C_5 = C_6 = 0$:

$$C_5 = 1P_9 + 1P_{10} + 1P_{12} + 1P_{15} + 1P_{17} + 1P_{18} + 1P_{19} = 0$$

$$C_6 = 1P_7 + 1P_{10} + 1P_{13} + 1P_{15} + 1P_{18} + 1P_{20} = 0$$

If positions 19 and 20 are chosen so that the above equations are always satisfied, then the final code word takes the form:

1 1 1 1 1	0 X X X X 0 X X X X 0 X X	P_{19} P_{20}	0	X X X X X X X X X X
Prefix		Parity		Check Bits

Operating as a ground-air command system, the above coding will provide words of 31 bits, of which 10 are information bits, and will result in a command dictionary of 2^{10} words.

It is of interest to determine a quantitative indication of the reliability of this link when operating in the error-detecting mode. This would be the most useful mode of operation for a command link, since there is always a return link via telemetry for requesting repeats of commands and for indicating verification.

As the link is not power-limited (ground to air), it is both conservative and reasonable to expect sufficient signal/noise ratio for an elemental error probability $p_e = 10^{-4}$. (Ref. 11) The probability of obtaining a word with a 5-bit error is thus (Ref. 12):

$$P_{31}(5) = C_5^{31} \; p_e^5 \; (1 - p_e)^{26}$$

$$P_{31}(5) = 1.7 \times 10^{-15}$$

The probability that such a word is contained in the code is simply:

$$\frac{2^{10}}{2^n} = 2^{-21}$$

The probability of an undetected word in error therefore becomes:

$$P(\omega) = 1.7 \times 10^{-15} \times 2^{-21} = 0.85 \times 10^{-21}$$

It may be more meaningful to express this in terms of the mean time between error which, for an assumed data rate of 1 megabit per second, becomes:

$$\Delta T = 10^{14} \text{ years.}$$

The link established between ground and vehicle has the reliability of communication stated above, as well as the same reliability of maintaining synchronization.

RANGE AND RANGE RATE

With the basic coded synchronous link established from ground to air, it is necessary to close the loop with a return link via a transponder aboard the vehicle in order to obtain range and range rate information. If the up-going coded bit sequence is transponded on the return air-ground path, then range can be derived from the sequence. Instead of employing correlation-detection techniques, as with pseudo-random noise sequences, it is sufficient to decode the sequence for the no-error condition, which corresponds to obtaining round-trip word synchronization. Since the code is designed "comma-free", the time to achieve this condition is again less than or equal to one word length. In practice, a selected word of the code can be transmitted, which would simultaneously start a count of the round-trip time for the word to traverse the loop. This initial word selection is employed to remove any possibility of range ambiguity. When a lock on the return sequence has been achieved, ranging information will be independent of the command dictionary used. Range rate or Doppler information is extracted from the signal carrier by employing standard techniques for this process. (Ref. 13,14, and 15)

CONCLUSIONS

The collection of the range, range rate, command, and synchronization functions within one reliable communication channel will make the Range group task of supporting the numerous programs more amenable to a reasonable and economic solution.

The ability to code commands such that their correct receipt is ensured is highly desirable in view of the cost of abortive missions. The system described has both the advantages of reliability and simplicity necessary for vehicular applications. The code words have a considerable degree of redundancy, which is used to obtain reliability.

The basic coded dictionary is not limited to the employment described here, but may be used wherever the requirement exists for extreme reliability of message transfer.

REFERENCES

(1) M. W. Williard, "PCM Telemetry Synchronization," Proceedings of the National Telemetry Conference, May 1961.

(2) M. W. Williard, "Optimum Code Patterns for PCM Synchronization," Proceedings of the National Telemetry Conference, May 1962.

(3) R. H. Baker, "Group Synchronization of Binary Digital Systems," Communication Theory, Willis and Jackson (Butterworth's Scientific Publications, 1953).

(4) J. P. Magnin, "Digital Synchronization of PCM Telemeters," Proceedings of the National Telemetry Conference, May 1962.

(5) E. N. Gilbert, "Synchronization of Binary Messages," IRE Transactions on Information Theory, Vol. IT 6, September 1960.

(6) J. J. Stiffler, "Synchronization of Telemetry Codes," IRE Transactions on Space Electronics and Telemetry, SET-8, June 1962.

(7) H. C. Crick, J. S. Griffith, and L. E. Orgel, "Codes Without Commas," Proceedings of the National Academy of Science, Vol. 43, 1957, pp. 416-421.

(8) S. W. Golomb, B. Gordon, and G. R. Welch, "Comma Free Codes," Canadian Journal of Mathematics, Vol. 10, 1958, pp. 202-209.

(9) Ibid. (5)

(10) R. C. Bose and D. K. Ray-Chaudhuri, "On a Class of Error Correcting Binary Group Codes," Information and Control, Vol. 3, 1960, pp. 68-79.

(11) J. G. Lawton, "Comparison of Binary Data Transmission Systems," Proceedings National Convention on Military Electronics, June 1958.

(12) P. M. Woodward, Probability and Information Theory with Applications to Radar (Pergammon Press, 1960).

(13) R. C. Payne and P. Painter, Jr., "Bit Synchronization and Data Regeneration Techniques," Proceedings of the National Telemetry Conference, Vol. 2, 1962.

(14) S. E. Craig, W. Fishbein, and O. E. Rittenback, "Continuous Wave Radar with High Range Resolution and Unambiguous Velocity Determination," IRE Transactions on Military Electronis, MIL-6, April 1962.

(15) W. Peterson, Error Correcting Codes (MIT Press and John Wiley & Sons, 1961).

APPENDIX A

CODE CONSTRUCTION

APPENDIX A

CODE CONSTRUCTION

The construction follows that of Bose and Ray-Chaudhuri. If $n = 2^{m-1}$, then there exists a 2t error detecting (n,k) binary group code with $k = 2^m - 1 - mt$. For the present example n = 31 and m = 5, resulting in a (31, 21) code which will detect 2t = 4 errors in any combination.

The roots of the irreducible polynomial $x^5 + x^2 + 1$ are elements of the Galois Field, GF (2^5), from which the following table of 31 non-zero vectors can be derived.

X^0	=	1							=	1 0 0 0 0	=	α_1
X	=		X						=	0 1 0 0 0	=	α_2
X^2	=			X^2					=	0 0 1 0 0	=	α_3
X^3	=				X^3				=	0 0 0 1 0	=	α_4
X^4	=					X^4			=	0 0 0 0 1	=	α_5
X^5	=	1		$+ X^2$					=	1 0 1 0 0	=	α_6
X^6	=		X		$+ X^3$				=	0 1 0 1 0	=	α_7
X^7	=			X^2		$+ X^4$			=	0 0 1 0 1	=	α_8
X^8	=	1		$+ X^2$	$+ X^3$				=	1 0 1 1 0	=	α_9
X^9	=		X		$+ X^3$	$+ X^4$			=	0 1 0 1 1	=	α_{10}
X^{10}	=	1				$+ X^4$			=	1 0 0 0 1	=	α_{11}
X^{11}	=	1	$+ X$	$+ X^2$					=	1 1 1 0 0	=	α_{12}
X^{12}	=		X	$+ X^2$	$+ X^3$				=	0 1 1 1 0	=	α_{13}
X^{13}	=			X^2	$+ X^3$	$+ X^4$			=	0 0 1 1 1	=	α_{14}
X^{14}	=	1		$+ X^2$	$+ X^3$	$+ X^4$			=	1 0 1 1 1	=	α_{15}
X^{15}	=	1	$+ X$	$+ X^2$	$+ X^3$	$+ X^4$			=	1 1 1 1 1	=	α_{16}

$$
\begin{array}{lllllll}
x^{16} = 1 + x + x^3 + x^4 & = 1\,1\,0\,1\,1 = \alpha_{17} \\
x^{17} = 1 + x + x^4 & = 1\,1\,0\,0\,1 = \alpha_{18} \\
x^{18} = 1 + x & = 1\,1\,0\,0\,0 = \alpha_{19} \\
x^{19} = x + x^2 & = 0\,1\,1\,0\,0 = \alpha_{20} \\
x^{20} = x^2 + x^3 & = 0\,0\,1\,1\,0 = \alpha_{21} \\
x^{21} = x^3 + x^4 & = 0\,0\,0\,1\,1 = \alpha_{22} \\
x^{22} = 1 + x^2 + x^4 & = 1\,0\,1\,0\,1 = \alpha_{23} \\
x^{23} = 1 + x + x^2 + x^3 & = 1\,1\,1\,1\,0 = \alpha_{24} \\
x^{24} = x + x^2 + x^3 + x^4 & = 0\,1\,1\,1\,1 = \alpha_{25} \\
x^{25} = 1 + x^3 + x^4 & = 1\,0\,0\,1\,1 = \alpha_{26} \\
x^{26} = 1 + x + x^2 + x^4 & = 1\,1\,1\,0\,1 = \alpha_{27} \\
x^{27} = 1 + x + x^3 & = 1\,1\,0\,1\,0 = \alpha_{28} \\
x^{28} = x + x^2 + x^4 & = 0\,1\,1\,0\,1 = \alpha_{29} \\
x^{29} = 1 + x^3 & = 1\,0\,0\,1\,0 = \alpha_{30} \\
x^{30} = x + x^4 & = 0\,1\,0\,0\,1 = \alpha_{31}
\end{array}
$$

By employing the above table, it is possible to write the following matrix of vectors in terms of powers of α_1, i.e.,

$$
M = \begin{Vmatrix} \alpha_1 & \alpha_1^3 \\ \alpha_2 & \alpha_2^3 \\ \vdots & \vdots^3 \\ \alpha_n & \alpha_n^3 \end{Vmatrix}
$$

Since the above vectors form a cyclic group, $X^{31} = X^0 = 1$,

$$M = \begin{array}{c} \begin{matrix} \alpha_i & & & & & \alpha_i^3 & & & & \end{matrix} \\ \left\| \begin{matrix} 1&0&0&0&0 & 1&0&0&0&0 \\ 0&1&0&0&0 & 0&0&0&1&0 \\ 0&0&1&0&0 & 0&1&0&1&0 \\ 0&0&0&1&0 & 0&1&0&1&1 \\ 0&0&0&0&1 & 0&1&1&1&0 \\ 1&0&1&0&0 & 1&1&1&1&1 \\ 0&1&0&1&0 & 1&1&0&0&0 \\ 0&0&1&0&1 & 0&0&0&1&1 \\ 1&0&1&1&0 & 0&1&1&1&1 \\ 0&1&0&1&1 & 1&1&0&1&0 \\ 1&0&0&0&1 & 0&1&0&0&1 \\ 1&1&1&0&0 & 0&0&1&0&0 \\ 0&1&1&1&0 & 1&0&1&0&0 \\ 1&0&1&1&1 & 1&1&1&0&0 \\ 1&1&1&1&1 & 1&0&1&1&1 \\ 1&1&0&1&1 & 1&1&0&0&1 \\ 1&1&0&0&1 & 0&0&1&1&0 \\ 1&1&0&0&0 & 1&1&1&1&0 \\ 0&1&1&0&0 & 1&1&1&0&1 \\ 0&0&1&1&0 & 1&0&0&1&0 \\ 0&0&0&1&1 & 0&1&0&0&0 \\ 1&0&1&0&1 & 0&0&0&0&1 \\ 1&1&1&1&0 & 0&0&1&0&1 \\ 0&1&1&1&1 & 1&0&0&0&1 \\ 1&0&0&1&1 & 0&0&1&1&1 \\ 1&1&1&0&1 & 1&1&0&1&1 \\ 1&1&0&1&0 & 0&1&1&0&0 \\ 0&1&1&0&1 & 1&0&1&0&1 \\ 1&0&0&1&0 & 1&0&0&1&1 \\ 0&1&0&0&1 & 0&1&1&0&1 \end{matrix} \right\| \end{array}$$

This matrix M can be reduced to normal form by employing the two operations:

a. Interchange of two rows or columns.

b. Replacement of the i^{th} column by the sum of the i^{th} and j^{th} column.

$$C = \left\| \begin{array}{cccccccccc}
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1
\end{array} \right\|$$

Now $C^* = \left\| C, I_{21} \right\|$ represents the generator matrix for the (31, 21) code words which can be derived by vector addition modulo 2 from the above rows.

The code is represented in systematic form for ease in coding. The 21 information bits can be completely arbitrary and are followed by the 10 check bits to make a 31-bit word. At the receiving end, the same shift register is employed. After the complete word is shifted into the register, the contents of the register should be all zeros if no detectable error occurred.

APPENDIX B

CODE GENERATION

APPENDIX B

CODE GENERATION

The Bose-Chaudhuri (31, 21) code can be implemented with an (n - k) stage shift register with appropriate feedback connections. For a Bose-Chaudhuri cyclic code, the generator polynominal is

$$g(X) = m_1(X), m_3(X), \cdots m_{2t-1}(X)$$

For the present case, 2t-1 = 3 and

$$g(X) = m_1(X), m_3(X)$$

$$m_1(X) = X^5 + X^2 + 1$$

$$m_3(X) = X^5 + X^4 + X^3 + X^2 + 1$$

$$g(X) = 1 + X^3 + X^5 + X^6 + X^8 + X^9 + X^{10}$$

The (n - k) = 10 stage shift register is employed with addition (modulo 2) feedback connections as determined by the above generator polynomial. The k symbols of the code are shifted into the register and simultaneously onto the communication channel. Upon completion of the shift of k symbols into the register, the gate G is opened and the contents of the register are shifted onto the communication channel. These last (n - k) symbols represent the check bits of the complete word.

DISTRIBUTION LIST

Address	No. of Copies
Commander Space Systems Division Air Force Systems Command Air Force Unit Post Office Los Angeles, California Attn: Technical Data Center	10
USAF Contract Support Detachment No. 3 Philco Corporation Western Development Laboratories Palo Alto, California	1
Philco Corporation Western Development Laboratories Palo Alto, California	78 + 1 reproducible
	89 + 1 reproducible